Security device for decoding compressed encrypted data has safe microcircuit in magnetic card separate from case and also includes decompression circuits

Patent Number: FR2782563
Publication date: 2000-02-25

Inventor(s): MORENO ROLAND
Applicant(s): MORENO ROLAND (FR)

Requested Patent: ☐ FR2782563
Application Number: FR19980010543 19980819
Priority Number(s): FR19980010543 19980819
IPC Classification: G06F19/00; G06F17/30; G06F1/00; H04H1/02; G11B20/10
EC Classification: G10H1/00R2C
Equivalents: AU5376499, AU5376599, ☐ WO0011867, ☐ WO0011868

Abstract

The receiving device (M) has a case with a slit for a magnetic smart card and has a number of decoding circuits (r3-r5). Data from the receiving antenna passes to a decompression circuit (r2). Signals then pass to a circuit (r1) for conversion and presentation of signals. The signals to be received may be produced by a transmitter with a signal producing circuit (e1) connected to a compressor (e2), a data packet separation circuit (e3) and a packet decoding circuit (e4) which may be connected to a transmitting antenna.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 782 563**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 10543**

(51) Int Cl[7] : **G 06 F 19/00**, G 06 F 17/30, 1/00, H 04 H 1/02, G 11 B 20/10

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 19.08.98.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 25.02.00 Bulletin 00/08.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *MORENO ROLAND* — FR.

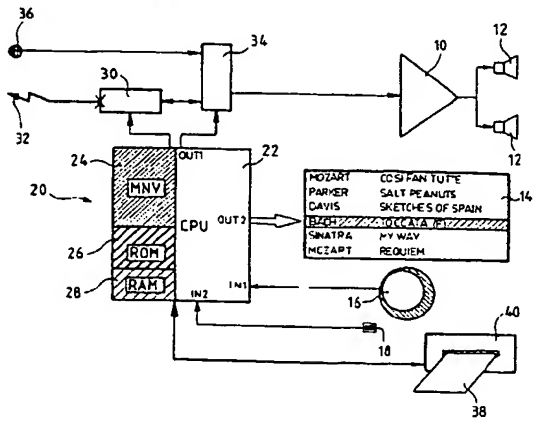
(72) **Inventeur(s) :** MORENO ROLAND.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET BARDEHLE PAGENBERG ET PARTNER.

(54) APPAREIL DE PRODUCTION DE SIGNAUX AUDIO POUR UNE INSTALLATION DE REPRODUCTION SONORE.

(57) Cet appareil comprend: des moyens téléinformatiques (20, 30; 30, 42), pour connecter l'appareil à un serveur distant, émettre vers ce serveur une requête de choix de plage sonore, et recevoir en réponse de ce site distant un flux de signaux numériques comprimés correspondant à la plage sonore choisie; et des moyens (20; 56) pour décomprimer le flux reçu et le transformer en un signal audio directement applicable à un amplificateur (10) de reproduction sonore. Avantageusement, l'appareil comprend en outre des moyens (50) de décryptage du flux de signaux numériques reçu et/ ou des moyens de réception d'au moins une liste de plages sonores, d'affichage (14) de tout ou partie de cette liste, et de sélection (16, 18) d'une plage dans la liste affichée; et/ ou des moyens de télépaiement (38), débités à réception du flux de signaux numériques depuis le serveur distant.



FR 2 782 563 - A1

La présente invention concerne un appareil formant source de signaux audio pour une installation domestique de reproduction sonore.

Ces installations peuvent fonctionner à partir de diverses sources, telles que des supports enregistrés (disques, bandes, etc.) ou transmises à distance (radiodiffusion).

Ces sources présentent toutes divers inconvénients :

- l'utilisation des supports enregistrés présuppose que l'utilisateur se soit au préalable déplacé pour les acheter ou les emprunter, avec bien entendu les difficultés qu'il peut rencontrer pour obtenir des enregistrements rares ou anciens, difficiles à trouver ;
- les sources radiodiffusées, quant à elles, présentent l'inconvénient d'un choix limité au nombre de stations captées par l'utilisateur, et de l'impossibilité de choisir le moment de début d'écoute, l'utilisateur étant astreint aux horaires de diffusion de la station qu'il reçoit.

L'un des buts de l'invention est de proposer une nouvelle source de signaux audio pour une installation sonore domestique, qui affranchisse l'utilisateur de ces inconvénients, en lui proposant :

- un très vaste choix de plages (morceaux musicaux),
- une possibilité de sélection des plages à volonté depuis l'installation,
- la possibilité du choix du moment de début d'écoute,
- l'absence de support matériel enregistré (donc gain de place et moindre coût de l'appareil du fait de l'absence d'éléments mécaniques),
- qualité sonore de type "numérique", c'est-à-dire très supérieure à celle des émissions radiodiffusées.

On verra par ailleurs que l'invention permet d'assurer le paiement des droits de diffusion aux divers éditeurs de musique en fonction du choix effectué par l'utilisateur, de la même manière que lorsque ce dernier achète un support d'enregistrement, et sans les inconvénients des paiements de droits par les radiodiffuseurs, qui ne tiennent pas compte, si ce n'est d'une façon statistique donc approximative, de l'audience réelle au moment de la diffusion de telle ou telle plage musicale.

Le point de départ de l'invention réside dans la constatation que les techniques modernes de compression des données rendent possible aujourd'hui la transmission du son, et particulièrement de la musique enregistrée, via un réseau téléinformatique (par exemple un réseau Internet) dans d'excellentes conditions techniques, c'est-à-dire compatibles avec le plus haut degré de qualité sonore aujourd'hui partout exploité (qualité générale dite "compact disc", avec échantillonnage à 44 100 kHz, sur 16 bits stéréo).

Ces possibilités sont en particulier offertes dans le cas d'une compression de type "MP3", avec un débit de l'ordre de 60 000 bps (bits par seconde) et, surtout, une vitesse de décompression identique à celle d'un modem couramment disponible aujourd'hui (56 000 bps). Des perspectives encore plus favorables peuvent même être envisagées avec des transmissions à plus grand débit telles que transmissions sur réseau RNIS ou sur réseau câblé, ou transmission de données numérisées par satellite sur les canaux à grand débit de télévision.

Plus précisément, la présente invention vise un appareil de production de signaux audio pour une installation de reproduction sonore, caractérisé en ce qu'il comprend : des moyens téléinformatiques, pour connecter l'appareil à un serveur distant, émettre vers ce serveur une requête de choix de plage sonore, et recevoir en réponse de ce site distant un flux de signaux numériques comprimés correspondant à la plage sonore choisie ; et des moyens pour décomprimer le flux reçu et le transformer en un signal audio directement applicable à un amplificateur de reproduction sonore.

Avantageusement, l'appareil comprend en outre :

- des moyens de décryptage du flux de signaux numériques reçu ; et/ou
- des moyens de réception d'au moins une liste de plages sonores, d'affichage de tout ou partie de cette liste, et de sélection d'une plage dans la liste affichée ; et/ou
- des moyens de télépaiement, débités à réception du flux de signaux numériques depuis le serveur distant, une information de titulaire de droits pouvant notamment être associée à chaque information de plage, de manière que le serveur puisse attribuer à leurs titulaires

respectifs les paiements correspondant aux plages choisies.

◊

On va maintenant décrire un exemple de mise en œuvre de l'invention, en référence aux dessins annexés.

La figure 1 est un schéma par blocs fonctionnels des différents éléments constituant l'appareil de l'invention.

La figure 2 est un schéma par blocs illustrant une variante de la figure 1, avec un degré d'intégration supérieur des éléments.

La figure 3 illustre les échanges de signaux entre les différents sites ou blocs intervenant dans la mise en œuvre de l'appareil de l'invention.

◊

Sur la figure 1, la référence 10 désigne une unité classique ampli/préampli stéréo alimentant une paire de haut-parleurs 12. L'unité 10 peut être soit intégrée à l'appareil de l'invention (qui se présente alors extérieurement sous la forme habituelle d'un amplificateur de chaîne haute fidélité) ou extérieure à celui-ci (l'appareil de l'invention se présentant alors sous forme d'un boîtier de même type qu'un lecteur de CD, tuner, etc. connecté à l'une des entrées d'un amplificateur classique).

L'appareil comprend de plus, de façon caractéristique, un afficheur 14 susceptible de présenter à l'utilisateur une série de plages musicales, ainsi que des moyens de sélection de ces plages musicales, par exemple sous forme d'une molette 16 (pour faire défiler les plages) combinée à un bouton-poussoir 18 de validation.

L'appareil comporte également un processeur programmable 20 comprenant essentiellement une unité centrale de traitement CPU 22 et une mémoire non volatile MNV 4, indépendamment de ses ressources propres en mémoires morte ROM 26 et vive RAM 28. Le processeur 20 reçoit les informations de sélection et de validation provenant de la molette 16 et du bouton-poussoir 18, et il pilote l'afficheur 14.

La mémoire non volatile 24 peut éventuellement incorporer un dis-

que dur de faible volume, si les contraintes techniques particulières en imposent la nécessité, ou être simplement constituée d'un "disque solide", c'est-à-dire d'une mémoire à semiconducteurs de grande dimension, par exemple 32 Mo.

L'appareil est également relié à un modem 30 chargé d'interfacer l'appareil avec le réseau téléphonique 32, typiquement à une vitesse de 56 000 bps.

L'appareil comporte également un circuit de commutation 34 permettant la sélection entre, d'une part, la réception d'une source audio par le modem 30 et, d'autre part, les autres entrées habituelles de l'amplificateur (CD, tuner, cassette, etc.) regroupées sur le dessin sous forme d'une entrée "auxiliaire" 36.

Le processeur 20 est en outre relié à une carte à puce 38, dont le rôle sera expliqué plus bas, par l'intermédiaire d'un lecteur 40.

L'utilisation de cet appareil a lieu essentiellement de la manière suivante.

A la mise sous tension, par exemple par appui sur le bouton 18, l'appareil se connecte automatiquement par le réseau téléphonique 32 à un site distant ou "site discothèque", dont l'adresse, Internet ou autre, est enregistrée de façon permanente dans la mémoire non volatile 24.

Le programme principal pilotant le processeur 20 permet alors la "navigation" sur ce site, ce programme incorporant par exemple un sous-ensemble d'un logiciel de navigation classique, spécialement adapté et simplifié pour les besoins du dispositif de l'invention.

L'utilisateur va ainsi naviguer dans un répertoire de plages musicales, qu'il pourra faire défiler et sélectionner au moyen de la molette 16 et du bouton-poussoir 18.

Le cas échéant, le système de navigation et l'afficheur pourront être adaptés pour faciliter l'accès par sélection de genres ou sous-genres musicaux, ou encore par sélection croisée entre genres musicaux (classique, jazz, opéra, etc.) et type d'œuvres (éditions originales, nouveautés, titres les plus/les moins demandés, etc.. L'afficheur 14 pourra alors se présenter sous forme d'un tableau à double entrée sélectionnable par des commandes appropriées en abscisse et en ordonnée (écran tactile, double rangée de boutons, etc.) permettant de désigner une intersection ligne/colonne.

Une fois la sélection de la plage musicale opérée, le processeur 20 adresse un ordre au site distant afin de permettre le téléchargement de la plage musicale choisie.

Ce téléchargement peut être opéré en temps réel (audition au fur et à mesure du chargement) ou quasi-réel, en prévoyant dans le processeur une mémoire tampon, par exemple pour accroître les performances de décompression et/ou de décryptage.

La carte à puce 38 est utilisée pour permettre un décryptage et/ou le paiement des droits attachés à l'œuvre musicale de la plage sélectionnée.

Dans ce cas, il est avantageux d'utiliser une structure telle que celle illustrée figure 2, présentant un degré d'intégration supérieur — et donc une plus grande sécurité à l'encontre des fraudes.

Les circuits de sécurité/décryptage/paiement sont inclus dans un bloc 42, avantageusement réalisé sous forme d'un ensemble monolithique, circuit intégré ou circuiterie hybride noyée dans un matériau de protection empêchant tout accès non destructif aux éléments du circuit.

Ce bloc 42 comporte un module SAM (*Security Access Module*) de carte à puce classique dans lequel pénètre le flux brut (c'est-à-dire crypté et comprimé) issu du modem 30, ce module 44 étant chargé de générer les clés 48 nécessaires au décryptage.

Le bloc 42 comporte également un module de décryptage 50 recevant le flux brut 52 et traitant celui-ci au moyen des clés 48 pour délivrer en sortie un flux 54 décrypté et comprimé.

Le bloc 42 comporte en outre un module de décompression 56, par exemple de type MP3 à 44,1 kHz, 16 bits stéréo, à une cadence compatible avec une écoute en temps réel, délivrant en sortie le flux de données décrypté et décomprimé 58 appliqué en entrée de l'amplificateur 10.

La carte 38 pourra également être utilisée pour le paiement des droits attachés à l'œuvre musicale, par des procédures télélogicielles connues telles que "cybercash", "virtual-money", etc.

Les données devant être échangées pour permettre ce paiement sont illustrées de façon schématique sur la figure 3.

Ce processus de paiement implique des échanges de signaux entre les points suivants :

- site "musical" SM, qui est un site Internet propre à l'éditeur de musique correspondant à la plage musicale choisie,
- site "corporatif" SC, commun aux divers éditeurs participant au système et chargé de répartir les droits entre ces derniers,
- mémoire non volatile MNV de l'appareil, pour le stockage temporaire des données,
- logiciel (soft) de l'appareil,
- carte à puce 38,
- amplificateur 10.

Les différentes étapes référencées 1 à 7 sur la figure sont les suivantes :

1. Le site musical SM correspondant à la plage sélectionnée par l'utilisateur envoie à l'appareil un fichier MP3, ou un bloc de données MP3, à l'appareil qui stocke ces informations dans sa mémoire non volatile MNV.
2. L'échange de données entre l'appareil et la carte à puce (flux 2 et 2') réalise le décryptage des données, opéré dans le bloc 50 de la figure 2.
3. L'appareil inscrit alors dans la mémoire de la carte à puce une information de débit, correspondant à la plage choisie et à l'éditeur de musique correspondant.
4. Le logiciel délivre alors à l'amplificateur, après les avoir décompressées, les données à écouter.
5. Simultanément, ou bien en temps différé, l'appareil se connecte au site corporatif SC.
6. L'information de débit stockée à l'étape 3 est alors transmise au site corporatif.
7. A intervalles réguliers, le site corporatif crédite l'éditeur de musique particulier des droits débités dans l'appareil.

Le débit peut être opéré par divers moyens connus : utilisation d'une carte prépayée (carte à décompte), d'une carte d'abonnement avec débit ultérieur de l'abonné, par exemple sur la facture qu'il reçoit de son fournisseur Internet, système de fidélisation, de plages gratuites promotionnelles, etc.

Le processus de paiement peut être résumé par l'algorithme en mé-

talangage suivant.

Amplificateur :

```
while counter> Max
     Exec (Payment_Process)
     Exec Receive_New_Key)
wend
Exec (Pay_Then_Decode)
END
```

Site distant :

```
Receive_Card_Counter
while Counter > Max
     Exec Payment_Process
wend
Download_Music
return
```

Payment_Process (amplificateur) :

```
Payment_Process_Protocol
if payment is NOT OK then END
Receive_New_Key
return
```

Payment_Process (site distant) :

```
Receive_Royalties_Data from Card
if Royalties_Data is NOT OK then END
Debit_Customer_Royalties_Sum
Credit_Publisher
Send_New_Key
set Card_Counter = Ø
return
```

Par ailleurs, dans une variante de réalisation on pourra exploiter les possibilités cryptographiques offertes par la combinaison de

trois données (ou sources de données) particulières :

- identité carte ;
- données d'exploitation (musique numérisée) ;
- germe aléatoire (fixe ou périodique).

Ainsi, la modulation peut-elle être rendue fonction d'une identité propre à l'amplificateur-client, c'est-à-dire indécodable par un intrus qui tenterait indûment de décoder les plages musicales qui ne lui sont pas destinées.

En outre, un tel dispositif permettrait une tarification proportionnelle à la durée d'écoute, dès lors que la périodicité du germe aléatoire pourrait être suffisamment brève. Par exemple : une unité de compte toutes les soixante secondes.

REVENDICATIONS

1. Un appareil de production de signaux audio pour une installation de reproduction sonore, caractérisé en ce qu'il comprend :

- des moyens téléinformatiques (20, 30 ; 30, 42), pour :
  - connecter l'appareil à un serveur distant,
  - émettre vers ce serveur une requête de choix de plage sonore,
  - recevoir en réponse de ce site distant un flux de signaux numériques comprimés correspondant à la plage sonore choisie,
- des moyens (20 ; 56) pour décomprimer le flux reçu et le transformer en un signal audio directement applicable à un amplificateur (10) de reproduction sonore.

2. L'appareil de la revendication 1, comprenant en outre des moyens (50) de décryptage du flux de signaux numériques reçu.

3. L'appareil de la revendication 1, comprenant en outre des moyens de réception d'au moins une liste de plages sonores, d'affichage (14) de tout ou partie de cette liste, et de sélection (16,18) d'une plage dans la liste affichée.

4. L'appareil de la revendication 1, comprenant en outre des moyens de télépaiement (38), débités à réception du flux de signaux numériques depuis le serveur distant.

5. L'appareil de la revendication 4, dans lequel une information de titulaire de droits est associée à chaque information de plage, de manière que le serveur puisse attribuer à leurs titulaires respectifs les paiements correspondant aux plages choisies.

FIG_1

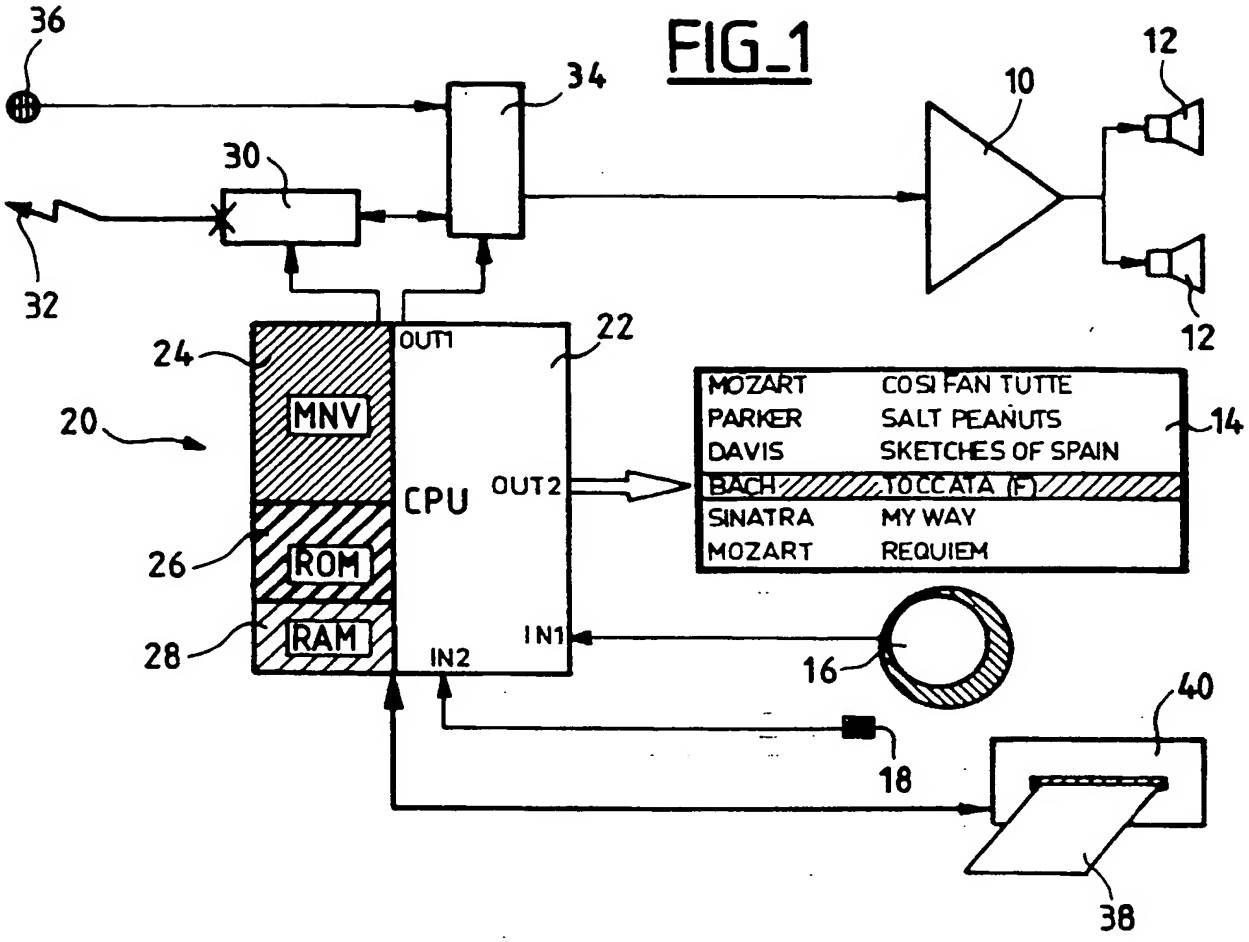

36
34
12
10
30
32
12
24
OUT1
22
MNV
20
CPU
OUT2
MOZART COSI FAN TUTTE
PARKER SALT PEANUTS
DAVIS SKETCHES OF SPAIN
BACH TOCCATA (F)
SINATRA MY WAY
MOZART REQUIEM
14
26
ROM
RAM
28
IN1
IN2
16
40
18
38

FIG_2

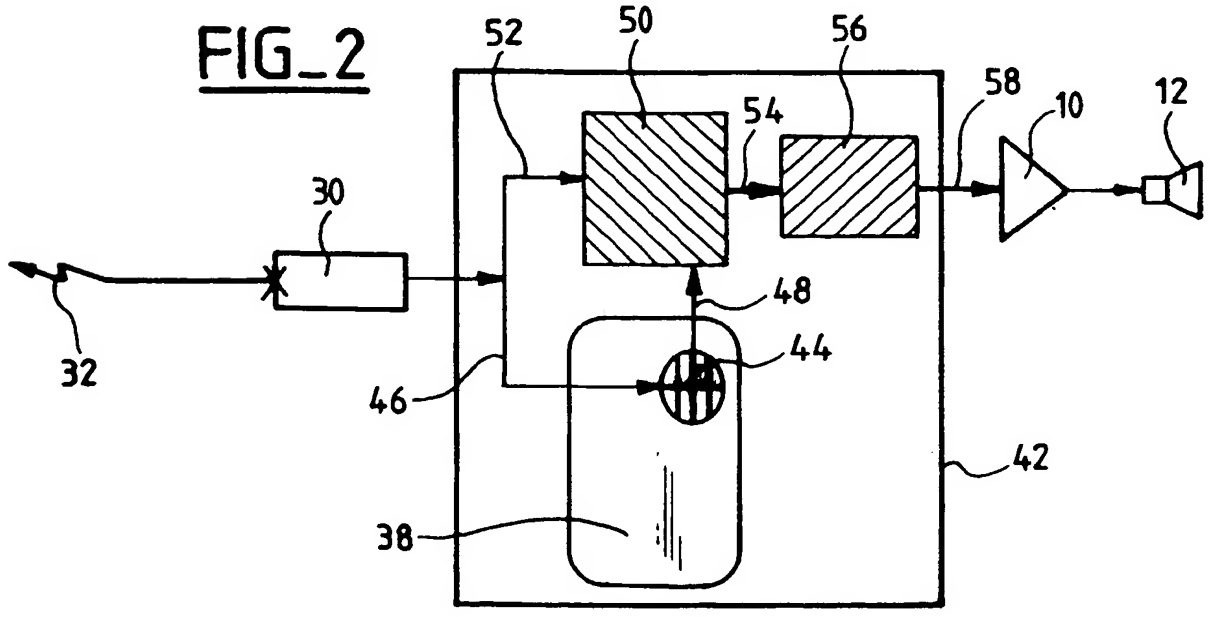
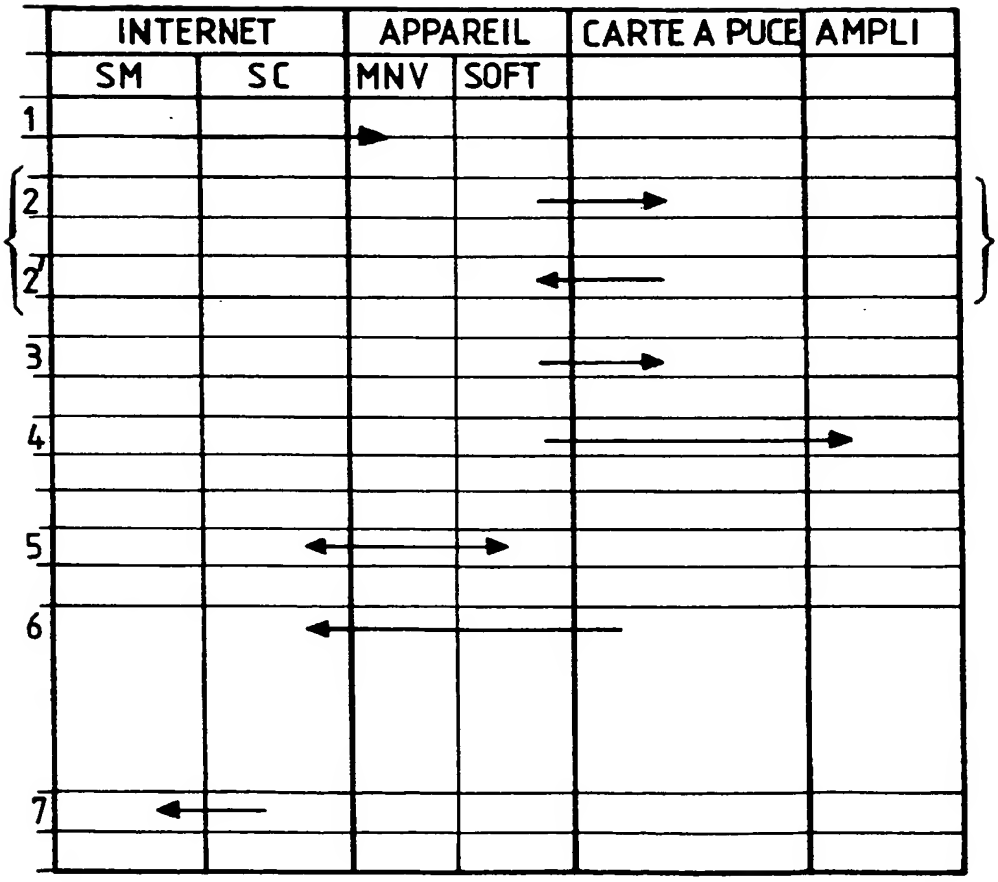

52
50
56
58
54
10
12
30
32
48
44
46
42
38

FIG_3



2782563

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 565080
FR 9810543

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	US 5 636 276 A (BRUGGER ROLF) 3 juin 1997 * colonne 1, ligne 17 - colonne 3, ligne 8 * * colonne 3, ligne 65 - colonne 5, ligne 59; figures 1,2 *	1-5
X	WO 96 12257 A (MASTRONARDI TONY ;NATHAN GUY (FR); TECHNICAL MAINTENANCE CORP (US)) 25 avril 1996 * page 5, ligne 26 - page 7, ligne 11 * * page 10, ligne 3 - ligne 6 * * page 21, ligne 4 - ligne 32 * * page 25, ligne 14 - ligne 27; figure 1 *	1-5
X	US 5 773 741 A (MILLS BRENT R ET AL) 30 juin 1998 * colonne 2, ligne 12 - ligne 33 * * colonne 5, ligne 51 - colonne 6, ligne 31 * * colonne 7, ligne 12 - ligne 56; figures 1,4 *	1-5

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G10H

Date d'achèvement de la recherche: 12 avril 1999

Examinateur: Pulluard, R

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

1